DART: Risk Management Case Study

Foreword: This Case Study is For You!

The DART project is a multi-faceted story with useful insights for Office of Chief Technologist (OCT) technology developers as well as new Human Exploration & Operations (HEO) Mission Directorate programs (Space Launch System, Multi-Purpose Crew Module, Commercial Crew and Cargo) confronting development, design verification and system-level testing challenges.

The Case Study is divided into two sections – the Case (this document) and the Epilogue (a separate document). The Case describes the DART mission and objectives along with a discussion of technical and project management issues, including the political and risk posture environment. The Case also includes a set of exercises and questions for individual consideration and/or group discussion. The Epilogue provides a discussion and assessment of the DART mission implementation.

1.0 Introduction

The Demonstration of Autonomous Rendezvous Technology (DART) mission was selected by NASA in 2001as a high-risk technology demonstration project to advance capabilities in automated rendezvous and proximity operations and advanced video guidance sensor technology. The goal was to move the technology from a readiness level (TRL) 4 to 7 - in other words, from component and/or breadboard validation in a laboratory environment to system prototype demonstration in a space environment. Ultimately DART was designated as a critical stepping stone in developing the capability to autonomously resupply the International Space Station (ISS).

Figure 1. Artist Concept – DART Mission Enabling Future Autonomous Resupply of International Space Station

2.0 Nominal Mission Plan

The intent of DART was to demonstrate that a pre-programmed and unaided spacecraft could independently rendezvous or meet up with a non-maneuvering and cooperating satellite. A series of 27 objectives for a successful mission were developed and divided among four defined mission phases. The four mission phases were as follows: 1) the launch and early orbit phase, 2) the rendezvous phase, 3) the proximity operations phase, and 4) the departure and retirement phase.

Launch and Early Orbit Phase

During the launch phase (see figure 1), the DART spacecraft, coupled with its Pegasus launch vehicle, would be flown to an altitude of 40,000 feet over the Pacific Ocean aboard a carrier aircraft. Following release, the three-stage Pegasus rocket would ignite, carrying DART into an initial parking orbit below MUBLCOM. From there, it would begin a series of navigation system checks, verifying position estimates for both itself and its target, MUBLCOM.

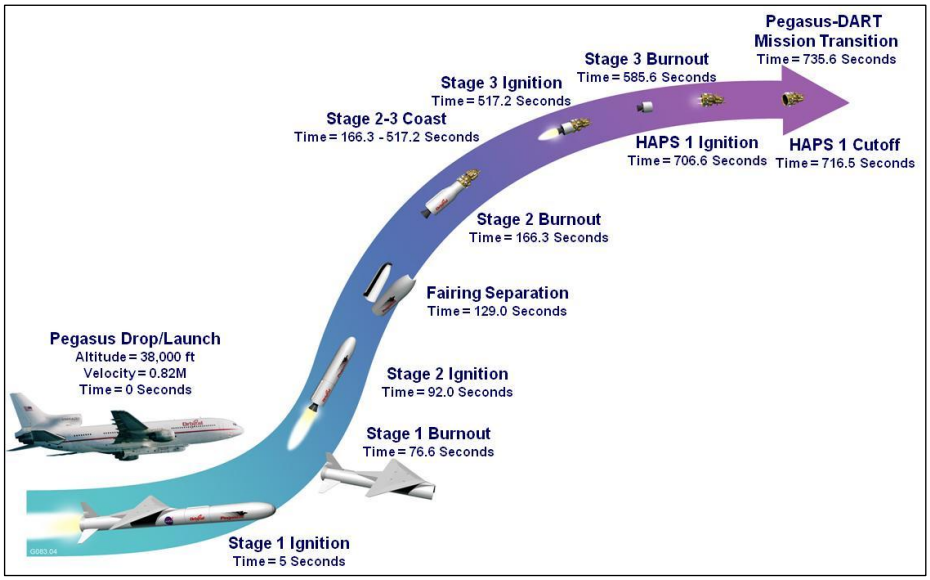


Figure 2. Nominal Launch Phase

Rendezvous Phase

During the mission's rendezvous phase, after completing the systems checks, DART would fire its HAPS thrusters to move into a second phasing orbit or rendezvous. The HAPS burn would be timed to specifically position DART below and behind MUBLCOM in preparation for the mission's next phase.
Among other things, NASA intended to demonstrate that a comparison of position and velocity data from GPS receivers in two spacecraft would be accurate enough to guide the "chaser" spacecraft (DART) to a position within the effective range of a proximity operations navigational sensor such as the AVGS.

Proximity Operations Phase

During the proximity operations phase, a series of scheduled maneuvers would move DART into MUBLCOM's orbit, first at a position about 3 kilometers behind, and then about 1 kilometer behind the target.

When it was 1 kilometer behind MUBLCOM, DART was programmed to evaluate AVGS performance through a series of precise, close-range maneuvers. These maneuvers included various pre-planned holds (station-keeping periods at designated points in space), a collision-avoidance maneuver at a pre-determined position, and a maneuver to determine at what distance from MUBLCOM the AVGS tracking data could no longer be acquired.

Departure and Retirement Phase

After completing its proximity operations maneuvers, DART would perform a departure burn (to move it away from MUBLCOM), expel its remaining fuel, and place itself into a short-lifetime retirement orbit in compliance with NASA safety standards.

3.0 The DART Spacecraft

Figure 3. DART Spacecraft

The DART spacecraft (see figures 3,4, and 5) was a combination of two systems. The forward segment contained DART-specific systems including a propulsion tank, reaction control system thrusters, batteries, communications equipment, and the Advanced Video Guidance Sensor (AVGS). The AVGS, the mission's primary sensor, would collect navigation data while DART was in close proximity to MUBLCOM. The aft portion of the DART spacecraft was the fourth stage of a Pegasus launch vehicle, and included an avionics assembly and the Hydrazine Auxiliary Propulsion System (HAPS). The AVGS would gather data from laser signals reflected off targets mounted on MUBLCOM, and use these signals to calculate relative bearing and range data; that is, the direction and distance from DART to MUBLCOM. When the DART-mounted AVGS was within 200-500 meters of MUBLCOM, it was expected to provide only bearing measurements. When the AVGS was within 200 meters of its target, it was expected to provide not only bearing, but also range and relative attitude (orientation of a spacecraft relative to an external reference)

data. Other navigational sensors that were to work in concert with the AVGS included two Global Positioning System (GPS) receivers on DART and a GPS receiver on MUBLCOM. DART would use data from these GPS receivers to determine position and velocity relative to MUBLCOM. Based on an intricate combination of data from all of its navigational sensors, on-board software would guide DART while it was in close proximity to MUBLCOM.

Critical sub-systems shown in figure 4 and discussed in figure 5 include:

- The flight computer which contains the mission profile, flight rule set, integrates the sensor input, performs the math, and directs the thrusters
- The reaction control system which provides the thrust to maneuver the spacecraft
- The IMU or inertial measurement unit that combines a classical Inertial Navigation System (INS) comprised of accelerometers aligned with each of the principal directional axes with a GPS unit. The GPS unit (referred to as the SIGI) provides corrections or updates to the INS position, velocity, acceleration solution which may drift or accumulate small errors over time.

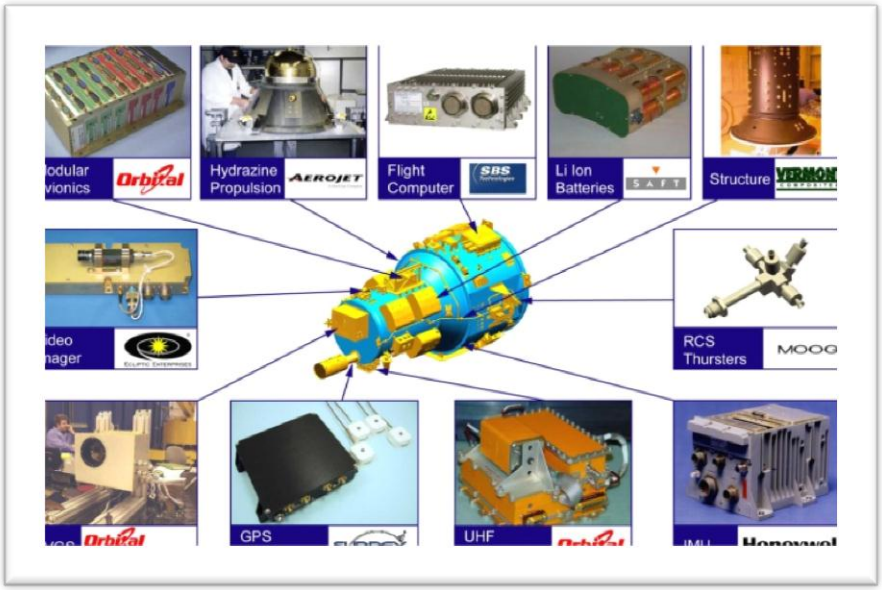


Figure 4. Critical Sub-Systems

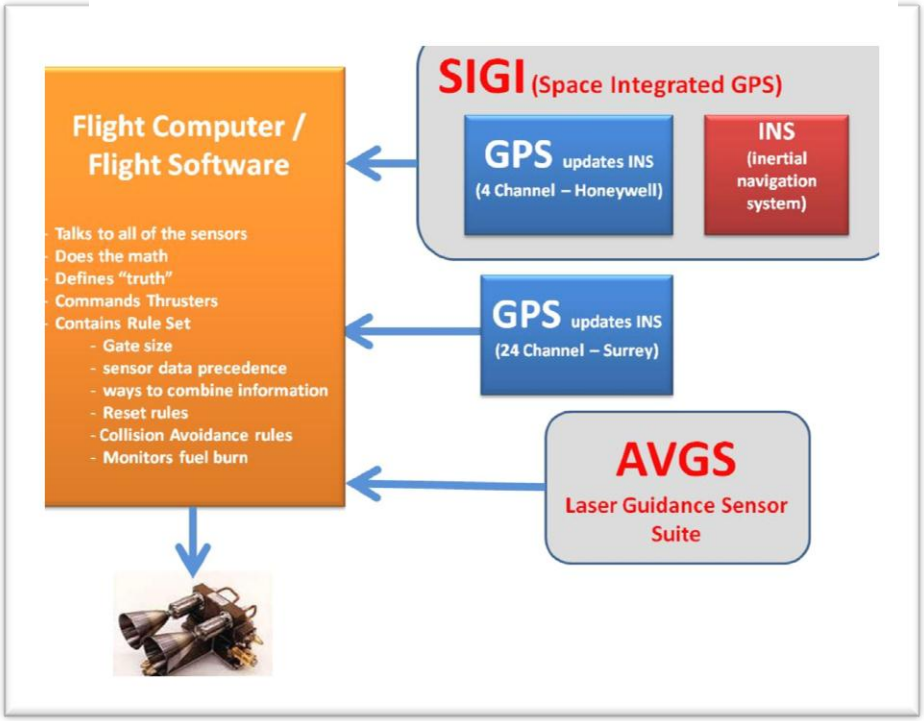


Figure 5. Navigation System Interactions

- The second GPS unit (referred to as the Surrey) which was added with the belief that it would provide more accurate information than the SIGI during on-orbit operations.
- The AVGS is the Advanced Video Guidance System that employs video imagery with algorithms to perform the necessary geometry to determine bearing and distance with great accuracy. The AVGS was intended for use within close proximity to the target vehicle.

4.0 Program Management Context

4.1 Contract

DART was proposed by Orbital Sciences Corporation (OSC) in response to a 2001 NASA Research Announcement from the 2nd Generation Reusable Launch Vehicle (2GRLV) Program. The DART contract was awarded in May 2001 to OSC. Regarding the contract value, The 2GRLV program flow is depicted in figure 6, providing a notional understanding of the successive down-selects strategy, progressing from many early candidates to the select few that become flight projects.

"Half of that (initial $47 M budget) was a fixed cost which was the Pegasus launch services, so we were developing, testing and flying a spacecraft for essentially 25 million dollars", stated DART's first project manager, Chris Calfee.

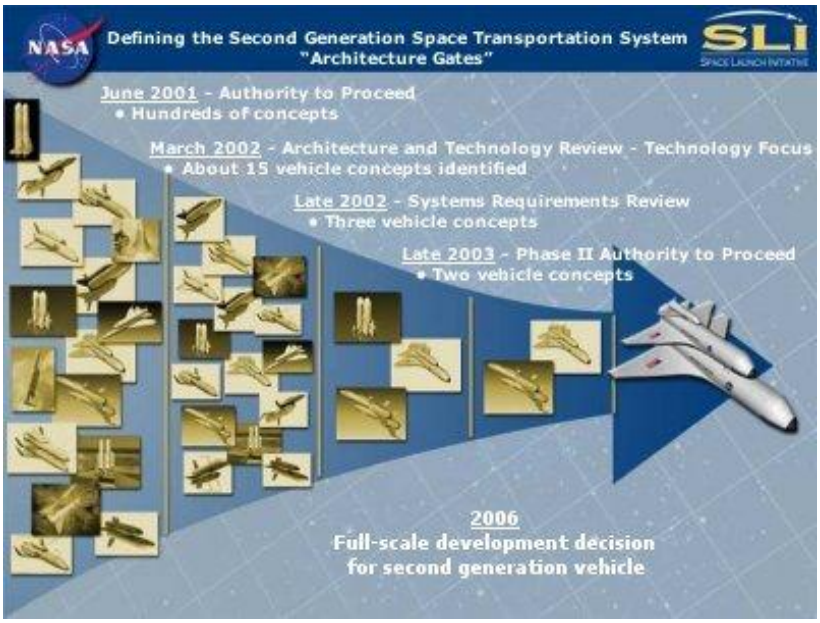


Figure 6. The 2nd Gen "Horse Race"

As a point of comparison – a hurricane-watch satellite mission cost $290 million while a. missile-warning satellite could cost between $682 million to one billion dollars. The NASA James Webb Space Telescope now has a price tag of $8.7 billion.

4.2 Governing Program Context

In November 2002, the 2GRLV Program was redefined and became two new programs, the Orbital Space Plane (OSP) Program and the Next Generation Launch Technology (NGLT) Program. DART, along with other flight demonstration projects, was transferred to the OSP Program. In the process, increased emphasis was placed on DART, because automated rendezvous technology was considered to be critical in supporting the potential future needs of the International Space Station Program. In January 2004, after President Bush announced the "Vision for Space Exploration" to explore the moon, Mars, and beyond and the OSP Program was cancelled. Because of its relevance to the in-space assembly of certain exploration architecture concepts, however, the DART project was continued. Due to the project's maturity at that time (its original, target launch date was scheduled for 2004), DART became NASA's first flight demonstration under the newly created Exploration Systems Mission Directorate. The DART mission was eventually launched on April 15, 2005, and cost 110 million dollars—109 % over the original contract value. Other changes occurred over DART's life-span (see figure 7) including three changes in the NASA Administrator (and attendant management philosophies), the Space Shuttle Columbia accident, and a change in management 18 months into the project – just after the Critical Design Review (CDR).

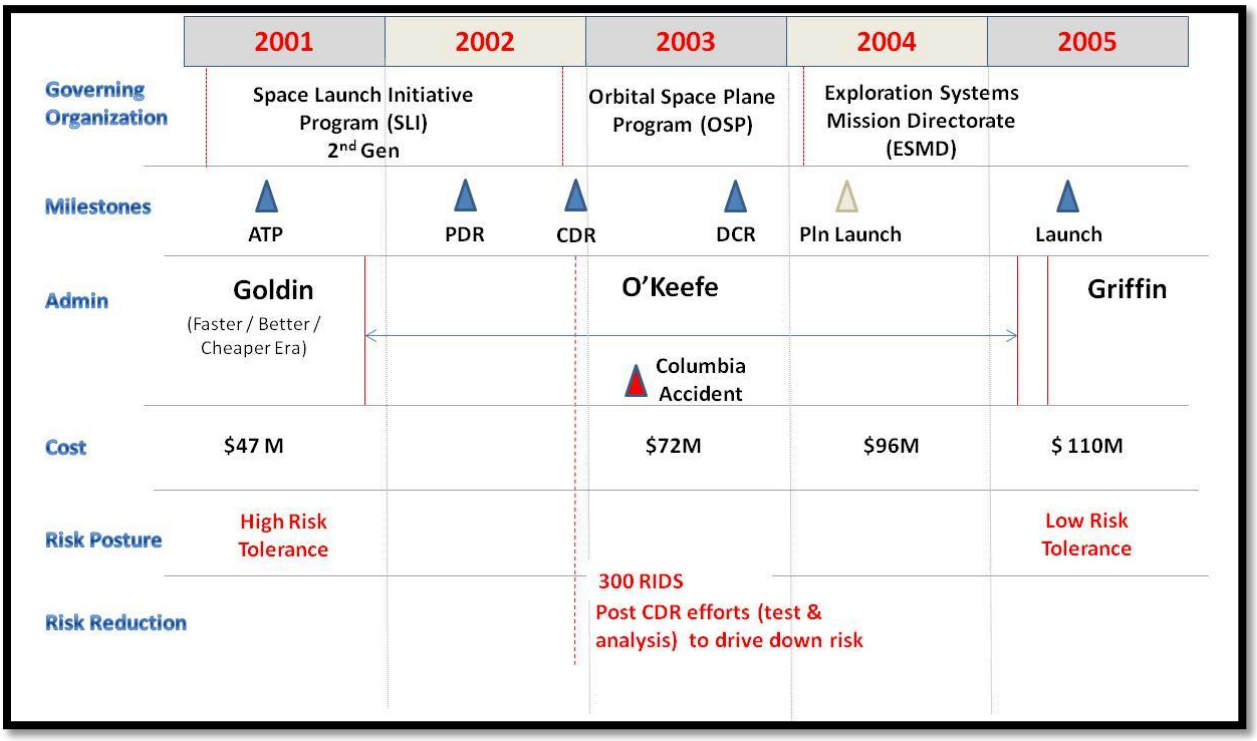


Figure 7. DART Implementation Context

5.0 Technical Issues

Ground Control

A topic of intense discussion and analysis early in the DART design phase was whether or not to add in ground command and control capability as a means to recover from unforeseen issues once on-orbit. Debate and discussions revolved around cost, scenario realism, and philosophy regarding risk acceptance for technology demonstration Class D missions. The project was proposed without ground commanding and as Chris Calfee recalled:

> *"it was very expensive to implement ground commanding, but the really biggest reason we chose not to was we didn't come up with a scenario that we really felt we could do something about it—could we actually get into a problem where we assess it, we get it fixed, and we upload the fix in time to save the mission? And we usually came back to no we likely could not even implement a fix even if we had the capability."*

Navigational System Design

Another major decision point in the DART design and development process involved whether or not to incorporate a second GPS receiver. The DART design team was concerned that the SIGI demonstrated reliability during launch phases might not have the required accuracy for on-orbit operations. As the team moved forward with the "Surrey" GPS integration a number of issues arose concerning technical performance. These concerns were exacerbated by communication restrictions with the U.K.-based vendor imposed by International Traffic in Arms Regulations (ITAR).

Heritage Software Design

The DART systems engineer Mark Krome identified concerns associated with building the DART command and control software within a heritage software operating environment.

> *One of the bigger challenges, from my perspective though, was that we were taking a heritage flight code that was that of the Pegasus flight computer and we were going to open that up and insert a whole new portion of flight code that would be the DART mission code, that I think involved a great deal of risk.*

Sometimes called a "Heritage Trap," efforts to leverage existing software and/or hardware designs may lead to unexpected outcomes.

Design Verification

As a low cost, high risk mission DART was implemented with a design verification approach that emphasized similarity and analysis rather than more expensive component and system level testing. Post-CDR, additional testing was introduced for selected components and a limited set

of simulated operational environments. While providing a degree of risk reduction (identifying latent defects in design, manufacturing and/or integration) the efforts did not meet the traditional Test-Like-You-Fly systems engineering philosophy employed for high cost, low risk missions.

6.0 Project Management Issues

Change in Risk Posture

As shown in Figure 6, the DART project spanned three separate programs (with changes in leadership each time), three separate NASA Administrators, Faster / Better / Cheaper philosophy, the Space Shuttle Columbia accident, the advent of the NASA Technical Authority, and attendant shifts in Agency culture and risk acceptance.

> *"Calfee noted that, "as time evolved—and really it wasn't an evolution that it changed, it was like it flipped overnight—DART suddenly went from a 'high risk, low cost' project to a can't fail, low cost project. Decisions were made early-on that really needed to be revisited, decisions were made early-on that you really could not undo, so that put the entire team in a difficult position."*

DART was, at the outset, clearly a Class D mission. Over time, expectations changed. The discussion in Appendix A compares and contrasts selected attributes of a Class D with Class B.

Staffing

Chris Calfee (former DART Project Manager)

> *"So June 2001 we got the Authority to Proceed and it was—as you can imagine with 22 contracts starting at once—there was a lot of confusion going on with respect to, 'Okay, who's the manager for this contract. How's it going to be organized?'*
> *So we hit the ground running without a real organization set up. So, I started recruiting people and it was interesting. I never really gained permission because there was really no one to gain permission from. So I started going out and recruiting people, and based on the project, I knew I needed supporting software and G&N (Guidance & Navigation). I knew I needed someone that could really help in conducting major reviews because we were laid out to have CDR by the end of 18 months. So I recruited about four people and one day I got a knock on the door that said, 'You know, you've exceeded your allotment of project personnel. You need to stop.' So I stopped and that was our project office: it was a four person team, really small."*

Aggressive Schedule to Manage Risk

The DART Project had some interesting schedule challenges from the risk management perspective. Certain events and conditions created schedule pressure (to hold down risk) while other events drove the need to delay and regroup (re-analyze, re-test), again, to drive down risk.

At the beginning of the DART project, "…it was a Twenty-two Project Horse Race," with the risk of cancellation looming large. DART was competing with 22 other mission candidates and had to move out very quickly just to survive the first 10 month "Termination Gate."

Chris Calfee (former DART Project Manager)

> *… the other part that is interesting about the way it was set up is there were gates implemented into all the SLI contracts; those gates allowed NASA to terminate if necessary without any repercussions. The gates were set at 10 – 12 month intervals—I don't think many people gave DART a chance of even getting past the first gate.*

The other condition driving the project forward was the very real possibility that the mission would "vaporize," (fundamental mission objectives required a target) if the rendezvous target, MUBLCOM became uncontrollable. The target had already exceeded its design life and had been displaying abnormal behavior in response to ground commands. A very real risk existed that the target might degrade to an unstable state pre-empting the rendezvous attempt.

Delays Accepted to Manage Risk

Notwithstanding the schedule pressures DART program management pulled back and accepted schedule delays to mitigate risk in two other areas related to mission success. First, the program accepted delays following the Critical Design Review (CDR) in order to accommodate additional testing. The DART CDR identified over 300 Review Item Discrepancies, or RIDs – problems that needed to be addressed. The response of management – given the changes in risk posture – was to delay for six months and add-in $50M of testing to drive down risk. The second case was immediately before the planned launch in November 2004. Just before the scheduled launch of DART the Pegasus launch vehicle identified a new (and higher) launch loads environment. DART had been designed and tested for a more benign set of load environments. Management decided to stand-down once again to conduct analyses necessary to ensure that structural design margins had not been compromised.

7.0 Case Exercise – Individual Study or Group Discussion

Two exercises are provided below for individual study and/or group discussion.

Risk Management Exercise:

The time is January 2003 – shortly after CDR. The DART Project had been shifted from 2nd Gen to the Orbital Space Plane (OSP) program. NASA senior management has announced that the DART Project is now a high priority, low risk mission - Class B. Over 300 problems and issues were identified in the critical design review – indicating potential risks and problems. The autonomous rendezvous and docking capability has been determined to be essential for commercial ISS resupply missions. Your job is to develop a briefing for senior management in which you:

- Identify top risk issues, proposed risk mitigation and control measures
- Propose risk mitigation and control activities
- Describe changes necessary in cost, schedule, and requirements baseline
- Provide other recommendations / requests that will ensure a high likelihood of mission success
- Recommend proceeding to the Design Certification Review or cancelling the mission

Risk Classification Exercise:

Using the appendices to the Case Study explore the attributes of the Agency payload risk classification approach and consider how it may (or may not) have been applied to the DART mission.

- Discuss and develop a team consensus on how DART would map into each of the classification categories at the outset of the project.
- What events that led to change in risk posture?
- What should have been done to document changes in management expectations?
- How do you think management would have mapped DART into each of the classification categories at the time of launch?
- Using Appendix B identify areas in which additional risk mitigation was implemented on the DART project post CDR.
- Would the additional risk mitigation measures be appropriate for future Technology Demonstration flight programs?

APPENDIX A: Payload Risk Classification

NASA NPR 8705.4, "Risk Classification for NASA Payloads (Revalidated July 9, 2008)," was designed to assist project teams in establishing a risk classification level (and project requirements) for their spacecraft and/or payload when flown on various types of launch systems. The document provides guidance on design and test philosophy and assurance practices applicable to each level.

The classification levels (A through D) define a hierarchy of risk combinations for NASA payloads by considering such factors as criticality to the Agency Strategic Plan, national significance, availability of alternative research opportunities, success criteria, magnitude of investment, and other relevant factors. Class A payloads would be equivalent to Hubble or the James Webb Space Telescope while Class D payloads tend to be low cost technology demonstrator missions.

A critically important point is provided in the 8705.4 introduction:

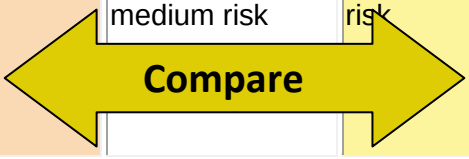
The establishment of the risk level early in the program/project provides the basis for program and project managers to develop and implement appropriate mission assurance and risk management strategies and requirements and to effectively communicate the acceptable level of risk.

The document sets the stage for the project execution addressing a myriad of requirements governing parts, material design – single point failures, analysis, software, verification testing, quality assurance, reviews, and risk acceptance level. NPR 8705.4, Appendices identify 8 classification considerations used to identify a payload class along with 15 assurance criteria and requirement areas.

8705.4 Appendix A - Classification Considerations for NASA Class A-D Payloads

Four risk levels or classifications have been characterized in Appendix A. The classification considerations in this appendix provide a structured approach for defining a hierarchy of risk combinations for NASA payloads by considering such factors as criticality to the Agency Strategic Plan, national significance, availability of alternative research opportunities or reflight opportunities, success criteria, magnitude of investment, and other relevant factors. Additional or alternate classification considerations may be applied to a specific payload or payload element. The importance weighting assigned to each consideration is at the discretion of the responsible Mission Directorate.

Characterization	Class A	Class B	Class C	Class D
Priority (Criticality to Agency Strategic Plan) and Acceptable Risk Level	High priority, very low (minimized) risk	High priority, low risk	Medium priority, medium risk	Low priority, high risk
National significance	Very high	High	Medium	Low to medium
Complexity	Very high to high	High to medium	Medium to low	Medium to low
Mission Lifetime (Primary Baseline Mission	Long, >5years	Medium, 2-5 years	Short, <2 years	Short < 2 years
Cost	High	High to medium	Medium to low	Low
Launch Constraints	Critical	Medium	Few	Few to none
In-Flight Maintenance	N/A	Not feasible or difficult	Maybe feasible	May be feasible and planned
Alternative Research Opportunities or Re-flight Opportunities	No alternative or re-flight opportunities	Few or no alternative or re-flight opportunities	Some or few alternative or re-flight opportunities	Significant alternative or re-flight opportunities
Achievement of Mission Success Criteria	All practical measures are taken to achieve minimum risk to	Stringent assurance standards with only minor	Medium risk of not achieving mission success may be	Medium or significant risk of not achieving mission success is

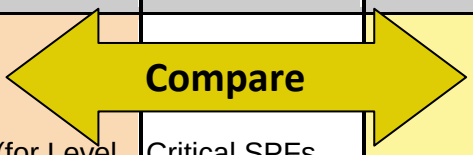


	mission success. The highest assurance standards are used.	compromises in application to maintain a low risk to mission success.	acceptable. Reduced assurance standards are permitted.	permitted. Minimal assurance standards are permitted.
Examples	HST, Cassini, JIMO, JWST	MER, MRO, Discovery payloads, ISS Facility Class Payloads, Attached ISS payloads	ESSP, Explorer Payloads, MIDEX, ISS complex subrack payloads	SPARTAN, GAS Can, technology demonstrators, simple ISS, express middeck and subrack payloads, SMEX

APPENDIX B: Assurance Provisions and Payload Classification

8705.4 Appendix B- Classification Considerations for NASA Class A-D Payloads

	CLASS A	CLASS B	CLASS C	CLASS D
Single Point Failures (SPFs)	Critical SPFs (for Level 1 requirements) are not permitted unless authorized by formal waiver. Waiver approval of critical SPFs requires justification based on risk analysis and implementation of measures to mitigate risk.	Critical SPFs (for Level 1 requirements) may be permitted but are minimized and mitigated by use of high reliability parts and additional testing. Essential spacecraft functions and key instruments are typically fully redundant. Other hardware has partial redundancy and/or provisions for graceful degradation.	Critical SPFs (for Level 1 requirements) may be permitted but are mitigated by use of high reliability parts, additional testing, or by other means. Single string and selectively redundant design approaches may be used.	Same as Class C.



Engineering Model, Prototype, Flight, and Spare Hardware	Engineering model hardware for new or modified designs. Separate prototype and flight model hardware. Full set of assembled and tested "flight spare" replacement units.	Engineering model hardware for new or significantly modified designs. Protoflight hardware (in lieu of separate prototype and flight models) except where extensive qualification testing is anticipated. Spare (or refurbishable prototype) hardware as needed to avoid major program impact.	Engineering model hardware for new designs. Protoflight hardware permitted (in lieu of separate prototype and flight models). Limited flight spare hardware (for long lead flight units).	Limited engineering model and flight spare hardware.
Qualification, Acceptance, and Protoflight Test Program	Full formal qualification and acceptance test programs and integrated end-to-end testing at all hardware and software levels.	Formal qualification and acceptance test programs and integrated end-to-end testing at all hardware levels. May use a combination of qualification and protoflight hardware. Qualified software simulators used to verify software and system.	Limited qualification testing for new aspects of the design plus full acceptance test program. Testing required for verification of safety compliance and interface compatibility.	Testing required only for verification of safety compliance and interface compatibility. Acceptance test program for critical performanc e parameters.
EEE Parts *http: // nepp .nasa .gov/ index_nasa .cfm/ 641	NASA Parts Selection List (NPSL)* Level 1, Level 1 equivalent Source Control Drawings (SCDs), and/or requirements per Center Parts Management Plan.	Class A requirements or NPSL Level 2, Level 2 equivalent SCDs, and/or requirements per Center Parts Management Plan.	Class A, Class B or NPSL Level 3, Level 3 equivalent SCDs, and/or requirements per Center Parts Management Plan.	Class A, Class B, or Class C requirement s, and/or requirement s per Center Parts Managemen t Plan.

Reviews	Full formal review program.Either IPAO external independent reviews or independent reviews managed at the Center level with Mission Directorate participation. Include formal inspections of software requirements, design, verification documents, and code.	Full formal review program.Either IPAO external independent reviews or independent reviews managed at the Center level with Mission Directorate participation. Include formal inspections of software requirements, design, verification documents, and peer reviews of code.	Full formal review program. Independent reviews managed at Center level with Mission Directorate participation. Include formal inspections of software requirements, peer reviews of design and code.	Center level reviews with participation of all applicable directorates. May be delegated to Projects. Peer reviews of software requirements and code.
Safety	Per all applicable NASA safety directives and standards.	Same as Class A.	Same as Class A.	Same as Class A.
Materials	Verify heritage of previously used materials and qualify all new or changed materials and applications/configurations. Use source controls on procured materials and acceptance test each lot/batch.	Use previously tested/flown materials or qualify new materials and applications/configurations. Acceptance test each lot of procured materials.	Use previously tested/flown materials or characterize new materials. Acceptance test sample lots of procured materials.	Requirements are based on applicable safety standards. Materials should be assessed for application and life limits.
Reliability NPD 8720.1	Failure mode and effects analysis/critical items list (FMEA/CIL), worst-case performance, and parts electrical stress analysis for all parts and circuits. Mechanical reliability, human, and other reliability analysis where appropriate.	FMEA/CIL at black box (or circuit block diagram) level as a minimum. Worst-case performance and parts electrical stress analysis for all parts and circuits.	FMEA/CIL scope determined at the project level. Analysis of interfaces. Parts electrical stress analysis for all parts and circuits.	Analysis requirements based on applicable safety requirements. Analysis of interface.

Fault Tree Analysis	System level qualitative fault tree analysis.	Same as Class A.	Same as Class A.	Fault tree analysis required for safety critical functions.
Probabilistic Risk Assessment NPR 8705.5	Full Scope, addressing all applicable end states per NPR 8705.5.	Limited Scope, focusing on mission-related end-states of specific decision making interest per NPR 8705.5.	Simplified, identifying major mission risk contributors.Other discretionary applications.	Safety only.Other discretionary applications.
Maintainability[1] NPD 8720.1	As required by NPD 8720.1	Application of NPD 8720.1 determined by program. (Typically ground elements only.)	Maintainability considered during design if applicable.	Requirements based on applicable safety standards.
Quality Assurance NPD 8730.5 NPR 8735.2 (NPR 8735.1)	Formal quality assurance program including closed-loop problem reporting and corrective action, configuration management, performance trending, and stringent surveillance. GIDEP failure experience data and NASA Advisory process.	Formal quality assurance program including closed-loop problem reporting and corrective action, configuration management, performance trending, moderate surveillance. GIDEP failure experience data and NASA Advisory process.	Formal quality assurance program including closed-loop problem reporting and corrective action, configuration management, tailored surveillance. GIDEP failure experience data and NASA Advisory process.	Closed-loop problem reporting and corrective action, configuration management, GIDEP failure experience data and NASA Advisory process. Other requirements based on applicable safety standards.

Software	Formal project software assurance program. Independent Verification and Validation (IV&V) as determined by AA OSMA.	Formal project software assurance program. IV&V as determined by AA OSMA.	Formal project software assurance program. IV&V as determined by AA OSMA.	Formal project software assurance insight. IV&V as determined by AA OSMA.
Risk Management NPR 8000.4	Risk Management Program. Risk reporting to GPMC.	Same as Class A.	Same as Class A.	Same as Class A.
Telemetry Coverage[2]	During all mission critical events to assure data is available for critical anomaly investigations to prevent future recurrence.	Same as Class A.	Same as Class A.	Same as Class A.